GRANTING STANDING IN DATA BREACH CASES: THE SEVENTH CIRCUIT PAVES THE WAY TOWARDS A SOLUTION TO THE INCREASINGLY PERVASIVE DATA BREACH PROBLEM

Clara Kim*

Data breaches at private companies have occurred with increasing regularity in recent years, causing the exposure and theft of confidential consumer data, such as credit card numbers. Despite these alarming patterns, the current state of the law does not fully regulate the complicated issues that arise from data breach incidents. The existing regulations operate in a piecemeal manner and do not adequately address the situation. They give inadequate protections to consumers and insufficient guidance to private companies that experience breaches and other institutions affected by data breaches, such as credit card companies and banks. This is the data breach problem: the increasing frequency of data breaches in recent years coupled with the lack of appropriate legal response.

Given the current situation, consumers are fighting back by filing class action lawsuits against private companies that have experienced data breaches. They have generally been unsuccessful, however, because many courts are reluctant to grant standing due to the lack of an identifiable injury, especially in cases where plaintiffs allege increased risk of future harm from misuse of their stolen personal information. This has especially been true after Clapper v. Amnesty International USA*, one of the most recent U.S. Supreme Court cases on Article III standing. Despite frequent*

* J.D. Candidate 2017, Columbia Law School; B.A. 2013, University of Chicago. The author would like to thank Lance Liebman for his invaluable guidance and encouragement and the staffers and editors of the *Columbia Business Law Review* for their help in preparing this Note for publication.

dismissals and confusion about Clapper*'s implications in the district courts, the Court of Appeals for the Seventh Circuit granted standing based on victims' reasonable allegations of increased risk of future harms in* Remijas v. Neiman Marcus Group, LLC.

This Note aims to demonstrate why the Seventh Circuit's approach is the best among the current decisions of the courts of appeals. Lessening the burden of standing requirements for consumer plaintiffs in data breach cases gives plaintiffs a potential avenue for relief, which is especially appropriate since there are inadequate regulatory and legislative mechanisms protecting consumers in data breach situations. In addition, the Seventh Circuit's approach is a step towards an ultimate solution, which this Note suggests should be in the form of comprehensive federal regulatory framework. The Seventh Circuit's approach allows for more cases to proceed to trial, and presumably for more companies to be held responsible for the consumer harm resulting from data breaches. This will allow for the responsibility for data security to be shifted to companies, which will hopefully shatter the current status quo and lead to a better solution. Though the Seventh Circuit's approach is appropriate given the current context, this Note recognizes that there are nonetheless a variety of complications in its practical application. These complications reveal the complexity of the data breach problem and lend further support to the proposition that the solution to the data breach problem will likely be regulatory, not judicial, in nature.

I. Introduction 546
II. The Data Breach Problem 548
A. The Prevalence of Data Breach Today.....548
B. Laws Governing Data Breach: State and Federal Laws 551
III. The Difficulty of Granting Standing in Data Breach Cases.....557
A. Article III Standing Requirements 557
B. Implications of *Clapper* for Meeting Standing Requirements 559

C. The Effect of *Clapper* on Data Breach Cases at the District Court Level 561
D. *Remijas*: The Seventh Circuit Case that Granted Standing in the Data Breach Context Post-*Clapper* 565
E. The Third Circuit: A Different Point of View 569
IV. The Seventh Circuit's Approach Should Be Followed, Despite Practical Complications 573
A. The Seventh Circuit's Approach Is a Step in the Right Direction 573
B. Finding Companies Negligent Without a Clear Understanding of What Negligence Means in This Context is Problematic 577
C. Holding Companies Responsible May Be Problematic When, in Some Cases, Hackings Are Serious Criminal Acts That the Company Could Not Have Reasonably Prevented 581
D. Holding Companies Liable May Actually Shift the Costs to Other Institutional Players 584
E. Holding Companies Liable Through the Court System Does Not Adequately Address Fundamental Considerations About Privacy 587
V. Conclusion 590

I. INTRODUCTION

Data breaches at private companies have occurred with increasing regularity in recent years. A data breach is "the loss, theft, or other unauthorized access . . . to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."[1] When data breaches occur at private companies, sensitive consumer data is often compromised and exposed. Despite this pattern, the current state of the law cannot fully address the complicated issues that arise from data breach incidents. The existing regulations operate in a piecemeal manner and do not

[1] 38 U.S.C. § 5727 (2012).

adequately address the situation. They give inadequate protections to consumers and inadequate guidance to private companies that experience breach and to other institutions affected by data breaches of private companies, such as credit card companies and banks.

Consumers are fighting back by filing class action lawsuits against companies that have experienced data breaches. They have generally been unsuccessful, however, because many courts are reluctant to grant standing due to the lack of an identifiable injury, especially in cases where plaintiffs allege increased risk of future harm from misuse of their stolen personal information. This has been especially true after *Clapper v. Amnesty International USA*,[2] one of the most recent U.S. Supreme Court cases on Article III standing. Despite frequent dismissals and confusion about *Clapper*'s implications in the district courts, the Court of Appeals for the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC* granted standing based on victims' reasonable allegations of increased risk of future harms.[3] This is not true of data breach actions brought in other circuits, however. In the Court of Appeals for the Third Circuit, for instance, the stringent standing requirements remain a barrier to litigation for data breach victims.[4]

The lack of appropriate legal redress for the increasingly common occurrence of data breaches described above is what this Note refers to as the "data breach problem." In order to address the data breach problem, this Note argues that an overarching federal regulatory framework is ultimately needed. However, the Seventh Circuit's decision is a step in the right direction, since conferring standing in data breach cases properly recognizes consumer harm in data breach situations. The Seventh Circuit's approach provides consumer plaintiffs a vehicle to address their injuries, which is especially important considering the lack of available regulatory or legislative remedies. In so doing, plaintiffs will

2 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

3 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

4 *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

be able to demonstrate the merits of their cases and the complexity of these issues to the courts, which will allow courts to rule in favor of plaintiffs in some instances. Hopefully, growing numbers of companies held liable without enforcement of clear standards for negligence will pressure the government to create an overarching regulatory solution. In other words, the Seventh Circuit's approach is one step—and the best one available thus far—towards solving the data breach problem.

In sum, this Note endeavors to show that the Seventh Circuit's approach is the best option among the courts of appeals' decisions, but also details potential complications in its application which further support the need for an ultimate regulatory solution to the data breach problem. Part II briefly summarizes the current state of the law on data breaches. Part III discusses judicial standing requirements, including an analysis informed by *Clapper v. Amnesty International USA*. In addition, the Note briefly analyzes the effect of *Clapper* in the district courts and introduces *Remijas v. Neiman Marcus Group LLC*, the first post-*Clapper* court of appeals decision on data breach. Lastly, Part IV argues that the Seventh Circuit's approach is the appropriate one given the current legal context and recognizes some of its practical complications in application. In conclusion, this Note argues that the Seventh Circuit's decision to put the onus for data protection on companies will hopefully shatter the current status quo and lead to a better solution to the data breach problem. This Note ultimately suggests that a comprehensive, federal regulatory framework is a possible solution to the data breach problem.

II. THE DATA BREACH PROBLEM

A. The Prevalence of Data Breach Today

Incidents of data breach in recent years include household names such as Michaels (2.6 million payment cards), Sally Beauty (280,000 credit and debit cards), New York State (22.8 million private records of New Yorkers

taken over eight years), Dairy Queen (600,000 debit and credit cards), Home Depot (56 million credit and debit cards), Jimmy John's (216 stores), JPMorgan Chase (76 million households and 7 million small businesses), and Sony (47,000 social security numbers, which were exposed more than 1.1 million times on 601 publicly-posted files stolen by hackers).[5] Data breaches now occur with increasing regularity and have become commonplace.[6]

Data breaches can occur in a variety of ways, but the case law of attempted and successful data breach class actions reflects three major categories: hacking, physical theft, and point-of-sale attacks.[7] Hacking is the type of data breach that people are probably most familiar with—essentially, it "involve[s] hackers accessing a company's network and stealing personal information."[8] Physical theft of company materials is another way data can be breached; this usually occurs when devices capable of data storage such as backup disks or laptops are stolen.[9]

Lastly, data can be stolen through point-of-sale attacks, generally associated with credit cards.[10] This can happen during the brief moment when an individual's credit card information is recorded and processed at the time of purchase. Though systems vary, generally when a customer gives credit card information to a merchant company for a transaction, the merchant company reads and stores the

5 Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015, 7:05 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/ [https://perma.cc/A469-97T4] (listing data breach incidents in 2014).

6 *See* Martin Giles, *Defending the Digital Frontier*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals [https://perma.cc/9PMR-L9UN].

7 Andrew Hoffman, *2 Years of Clapper: Takeaways From 12 Data Breach Cases*, LAW360 (Feb. 25, 2015, 5:13 PM), http://www.law360.com/articles/621745/2-years-of-clapper-takeaways-from-12-data-breach-cases [https://perma.cc/SE4N-XY8Q].

8 *Id.*

9 *Id.*

10 *Id.*

card information necessary to initiate the transaction.[11] This information is transmitted to the merchant's acquiring bank, and the bank will use the information to verify the customer's account balance through a high-speed credit card network (such as Visa or MasterCard) to ensure the customer has enough money or credit to advance the draw needed to complete payment.[12] In some systems, such as with American Express or Discover, these steps are merged into one, since these companies are "single card-issuing institutions with a direct relationship with the merchant."[13] Through this process, the card's information is transmitted from the consumer to the merchant company, from the merchant company to the merchant company's acquiring bank, and then again through the credit card network back to the card-issuing bank.[14]

If any institution at any step of this long chain of transactions is compromised, consumers' data may be exposed.[15] In addition, this chain of custody raises complex legal questions about who is obligated to whom. The contractual obligations are muddled when data is passed along multiple relationships: "card-issuing bank–customer, customer–merchant, merchant–acquirer bank, acquirer bank–card network, card network–card-issuing bank, or in the alternative, card-issuing bank–customer, customer–merchant, and merchant–integrated card network bank."[16]

Though the number of data breaches of private companies continues to grow with alarming speed, the law has not yet adequately addressed this issue. This is what is referred to as the "data breach problem" in this Note—the increasing frequency of data breaches in recent years coupled with the lack of appropriate legal response. Part II.B will demonstrate

11 R. Andrew Patty II, *Credit Card Issuers' Claims Arising From Large-Scale Data Breaches*, 23 J. TAX'N REG. FIN. INSTRUMENTS 5, 5, 8 (2015).

12 *Id.*

13 *Id.*

14 *Id.*

15 *Id.*

16 *Id.*

how the complexities described above play out on the current legal landscape.

B. Laws Governing Data Breach: State and Federal Laws

The legal issues that arise in data breach cases, such as determining who is at fault, the appropriate standards, and the remedy, are governed by a variety of laws from different law-making authorities.[17] The applicable laws for any given situation generally come from both the state and federal governments.[18] Some of these laws address issues specific to data breaches and the attendant increased risk of fraudulent use of stolen information, while others generally govern the protection and storage of information by private companies.[19] Any given data breach situation is subject to an array of regulations, but the lack of standardization or enforcement of these measures is alarming. Considering how pervasive and serious the data breach problem has been over the past few years, the current regulatory scheme is an untenable state of affairs.

After a data breach occurs, a company generally takes steps to remedy the situation, and these steps depend on the laws or regulations applicable to the specific situation. Currently, there are many different relevant law-making authorities, each playing a critical but confused role in attempting to solve the problem. First, companies have to follow state data breach notification laws, which vary from

17 *See* U.S. CHAMBER INST. FOR LEGAL REFORM, THE NEW LAWSUIT ECOSYSTEM: TRENDS, TARGETS AND PLAYERS 102–03 (2013), http://www.instituteforlegalreform.com/uploads/sites/1/web-The_New-Lawsuit-Ecosystem-Report-Oct2013_2.pdf [https://perma.cc/GGP2-57HG]; *see also* ADVISEN, THE LIABILITY OF TECHNOLOGY COMPANIES FOR DATA BREACHES 4 (2010), https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf [https://perma.cc/2X32-RM8A] (indicating that there is no uniform standard for data security).

18 *See* Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1178, 1181 (2014).

19 *See* Patty, *supra* note 11, at 8–9.

state to state.[20] As of December 2015, forty-seven states had data breach laws.[21] The existing state laws impose different requirements, some mandating that companies under certain circumstances inform their customers that their personal information may have been exposed due to a data breach within a certain amount of time.[22]

Second, companies must also comply with numerous federal laws. The federal law framework is more industry-related than consumer-oriented.[23] One of the best examples of this is the Health Insurance Portability and Accountability Act ("HIPAA"), which protects healthcare information by imposing data protection requirements upon relevant actors, such as healthcare and health plan providers.[24] Though extensive, HIPAA exclusively applies to specific healthcare information because it protects only

20 *See* Peters, *supra* note 18, at 1174–75.

21 Alabama, New Mexico, and South Dakota are the only states that did not have data breach laws as of December 2015. *See 2015 Security Breach Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Dec. 31, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx#2015 [https://perma.cc/7ZAU-K3BM]; *see also* Peters, *supra* note 18, at 1181 & n.71.

22 *See* Peters, *supra* note 18, at 1181–83.

23 *See id.* at 1181; *see also* Adam R. Foresman, Note, *Once More Unto the [Corporate Data] Breach, Dear Friends*, 41 J. CORP. L. 343, 346 & n.25 (2015) (describing the "sectoral" approach of federal law, which breaks down laws according to type and use of data, and citing U.S. CHAMBER INST. FOR LEGAL REFORM, *supra* note 17, at 102).

24 Health Insurance Portability and Accountability Act of 1996, 42 USC § 1320d (2012); *see also The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/privacy/ [https://perma.cc/7TW3-T2XB] ("The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.").

"individually identifiable health information."[25] While there are other applicable federal laws on data security, they do not directly address the issue at hand—where data breaches at private companies cause consumer information to be exposed and maliciously used in fraudulent ways. In addition, these laws are not often utilized to help protect consumers.[26] The existing federal laws that could potentially provide private rights of action against corporations are subject to a variety of limitations and exceptions that render them toothless. For example, the Computer Fraud and Abuse Act ("CFAA") provides a civil cause of action that could theoretically be utilized in a typical data breach case.[27] However, this cause of action has rarely been successfully used to protect consumer victims of data breaches because it requires a showing of substantial economic harm in order to be applied to a typical data breach case.[28]

---

25 Health Insurance Portability and Accountability Act of 1996 § 262(a), 42 U.S.C. §§ 1320d(6), 1320d-6(a) (2012); U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 3 (2003), http://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/5NWS-CV3C]; *see also* Peters, *supra* note 18, at 1179–80.

26 *See, e.g.*, P. Scott Ritchie, *Security Breach Cases Under Federal Law: A Brief Analysis*, CLAUSEN MILLER PC (Sept. 2013), http://www.clausen.com/index.cfm/fa/firm_pub.article/article/5e850e7a-9245-44b6-b87a-ca722a622d10/Security_Breach_Cases_Under_Federal_Law_A_Brief_Analysis.cfm [https://perma.cc/E6HH-8X7R].

27 18 U.S.C. § 1030(g) (2012).

28 18 U.S.C. § 1030(c)(4)(A)(i) (2012); *see also* Peters, *supra* note 18, at 1178. There are five different ways to bring a civil action under this statute. *See* 18 U.S.C. § 1030(g) (2012) (referring to 18 U.S.C. § 1030(c)(4)(A)(i)(I)–(V)). However, only the first situation is facially applicable to a typical data breach situation ("loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value"). Even so, proving damages of $5000 or more is generally not possible in most consumer data breach cases. The other four situations that allow for civil action are generally inapplicable to a typical consumer data breach situation in which data is stolen from a compromised merchant company: (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; and (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the

In addition, there is a scattered regulatory scheme in place as well by agencies such as the Securities and Exchange Commission ("SEC") and the Federal Communications Commission ("FCC").[29] The federal government has not yet released a manual or comprehensive set of regulations to help corporate management navigate all of the relevant cybersecurity and data security recommendations and requirements across all federal agencies.[30] In short, these laws cause confusion because the current state of affairs is a patchwork of laws that have been created to meet discrete needs within the larger data breach problem. Moreover, it is clear that the current limited regulatory systems are ill suited for the fast-changing nature of data breach, typical of problems intertwined with technological innovations.

The major federal agencies that give guidance regarding data security preparedness for most corporations include the SEC, the Federal Trade Commission ("FTC"), the FCC, the Department of Justice ("DOJ"), and the Department of Homeland Security ("DHS").[31] None of these guidelines are mandatory, but they help acquaint corporate boards to the standards their corporations should meet by communicating the preferences of government regulators.[32] A Commissioner of the SEC referred to the "Framework for Improving Critical Infrastructure Cybersecurity," released by the National Institute of Standards and Technology ("NIST") in February 2014, as a reference for corporate boards.[33] In

administration of justice, national defense, or national security. *See* 18 U.S.C. § 1030(c)(4)(A)(i) (2012).

[29] Thad A. Davis, Michael Li-Ming Wong & Nicola M. Paterson, *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 629 (2015).

[30] *See id.* at 627.

[31] *See id.* at 629.

[32] *See id.* at 627.

[33] *Id.* at 630; *see also* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf [https://perma.cc/GBE9-3H37].

addition, the SEC's Office of Compliance Inspections and Examinations released a sample list of requested information that it plans to use in cybersecurity investigations.[34] Although these guidance documents are not mandatory, agencies such as the SEC are signaling that companies should follow these rules in order to be viewed favorably if they become the subject of an investigation.[35] The SEC's actions impact the way plaintiffs structure their suits and how corporations operate. Essentially, though not enforced as mandatory, the SEC's guidance documents have an impact in the larger corporate field.[36]

In 2006, the FTC created the Division of Privacy and Identity Protection ("DPIP") to protect consumer data.[37] This is most relevant in the context of big data collection. The DPIP has ordered companies to establish and maintain privacy protection programs and procedures and has settled enforcement actions with several big companies.[38] In addition, the FTC released its own data security compliance guidelines in 2007, entitled "Protecting Personal Information: A Guide for Business."[39]

Contrastingly, the FCC has not attempted to set industry standards like the SEC and the FTC. However, due to the scope of its regulatory powers, the FCC was involved in a major case against two telecommunications companies in October 2014 for their failure to secure the private data of private individual customers.[40] The FCC announced a $10 million fine for the companies in that case.[41]

---

34 *See* Davis et al., *supra* note 29, at 630.

35 *See id.* at 631.

36 *See id.* at 632.

37 *Id.*

38 *Id.*

39 *Id.* at 633; *see also* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf [https://perma.cc/SD6H-8AC5].

40 Davis et al., *supra* note 29, at 634–35 & n.59.

41 *Id.*

The DOJ also plays a role in prosecuting criminals in data breach cases, shaping cybersecurity legislation, and working with the private sector in the data security realm.[42] In 2014, the DOJ took its first steps into the cybercrime world by establishing its Cybersecurity Unit.[43] It remains to be seen what role the DOJ will play—because of jurisdictional issues, federal prosecutors cannot effectively go after criminals working abroad who are hacking and trading the personal information of Americans stolen from American companies.[44] The best they can do is issue a notice, or in some cases, an arrest warrant, to the international community and petition for extradition, which can sometimes bring a criminal defendant into the United States for trial.[45] In recent months, the DOJ Cybersecurity Unit, in partnership with DHS, has been actively giving guidance in the cybersecurity realm.[46] Some of their recommendations provide protections for private companies that share information about potential threats with the federal government, which may be applicable in certain data breach cases.[47]

Lastly, DHS is also involved in this field in a limited way, by recognizing the importance of data security in the context of national security. DHS announced its intent to enhance cooperation and coordination with the private sector, given

42 *Cybersecurity Unit*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/criminal-ccips/cybersecurity-unit [https://perma.cc/4RN7-HRPG] (last updated Feb. 25, 2016).

43 Davis et al., *supra* note 29, at 635 & n.61.

44 *See, e.g.*, Press Release, U.S. Dep't of Justice, Office of Public Affairs, Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States (Feb. 17, 2015), http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states [https://perma.cc/H3KS-BKPD].

45 *See, e.g.*, *id.*

46 This is specifically with regard to the Cybersecurity Information Sharing Act of 2015. *See Automated Indicator Sharing (AIS)*, U.S. DEP'T OF HOMELAND SECURITY: U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/ais [https://perma.cc/5D3J-6HMQ].

47 *Id.*

that the private sector owns and operates over eighty-five percent of the nation's critical cyber infrastructure.[48]

III. THE DIFFICULTY OF GRANTING STANDING IN DATA BREACH CASES

A. Article III Standing Requirements

In order to bring a lawsuit in federal court, a plaintiff must have standing. In data breach cases, many plaintiffs have not been able to meet the standing requirement. District courts across the country have often imposed a high bar, often dismissing these cases before they even get through the door.

The standing requirement comes from Article III of the U.S. Constitution.[49] In order to bring a "case or controversy" in a federal court, the plaintiff must satisfy three elements of standing:

> First, the plaintiff must have "suffered an 'injury in fact'—an invasion of a legally protected interest." The injury complained of must be "actual or imminent, not 'conjectural' or 'hypothetical.'" Second, a plaintiff's claim must arise from an injury that "fairly can be traced to the challenged action of a defendant." Third, a favorable court decision must be able to redress the plaintiff's injury. The plaintiff bears the burden to establish all three elements.[50]

In data breach cases, the most difficult element to establish is the "injury in fact" requirement. First of all, many courts will not recognize that there is an injury at all for the individual consumer in data breach cases because many credit card companies and financial institutions will refund and void fraudulent purchases up to a point as a

48 Davis et al., *supra* note 29, at 637 & n.68.

49 U.S. CONST. art. III, § 2.

50 Patricia Cave, Comment, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 772 (2013) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)).

matter of industry practice. Since the individual consumer technically may not face monetary harm, courts have had a difficult time identifying a cognizable injury.[51]

In addition, courts are wary of claims about possible future injury. Generally, district courts have not recognized consumer complaints about the increased threat of identity theft.[52] However, the Courts of Appeals for the Seventh and Ninth Circuits have found standing due to the increased threat of future harm in some cases.[53] Two notable cases in these circuits are *Pisciotta v. Old National Bancorp* and *Krottner v. Starbucks Corporation*.[54] In *Pisciotta*, a class action suit against a bank, the Seventh Circuit found that "an act which harms the plaintiff only by increasing the risk of future harm" was sufficient to confer standing when the increase in risk was caused by the defendant's actions.[55] Thus, "[o]nce the plaintiffs' allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry."[56] More recently, in *Krottner*, the Ninth Circuit held that, though the court had not previously evaluated the increased risk of future identity theft as injury-in-fact, the situation was analogous to other contexts where the possibility of future harm was sufficient

51 *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., No. 14-CV-4787, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014), *rev'd and remanded*, No. 14-3700, 2016 WL 1459226 (7th Cir. Apr. 14, 2016) ("In order to have suffered an actual injury, Plaintiffs must have had an unreimbursed charge on their credit or debit cards."); *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 527 (N.D. Ill. 2011) ("Michaels is correct that Plaintiffs suffered no actual injury under the ICFA if Plaintiffs were reimbursed for all unauthorized withdrawals and bank fees and, thus, suffered no out-of-pocket losses.").

52 *See* Cave, *supra* note 50, at 774.

53 Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); *see also* Cave, *supra* note 50, at 774 & n.62.

54 *Pisciotta,* 499 F.3d at 629; *Krottner*, 628 F.3d at 1139; *see also* Cave, *supra* note 50, at 775.

55 *Pisciotta*, 499 F.3d at 634.

56 *Id.*

to meet standing requirements.[57] In *Krottner*, a laptop, containing the "unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees," was stolen from Starbucks.[58] The Ninth Circuit considered the increased risk of identity theft enough to constitute injury-in-fact.

Since these cases were decided, however, the Supreme Court decided a major case on standing, *Clapper v. Amnesty International USA*.[59] Some courts have taken the view that *Clapper* increased the stringency of standing requirements, foreclosing standing for plaintiffs alleging increased risk of identity theft. Others distinguish *Clapper* on its unique factual situation.[60] Regardless of what the "correct" interpretation of its holding is, *Clapper* has undoubtedly affected how district courts evaluate plaintiffs' claims in data breach class actions.

B. Implications of *Clapper* for Meeting Standing Requirements

In *Clapper*, plaintiffs attempted to bring a claim challenging Section 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA").[61] The plaintiffs were lawyers, human rights researchers, and journalists who were working with a particular clientele that could be subject to surveillance under FISA.[62] Section 702 of FISA ("§ 1881a") allows the government to obtain foreign intelligence information on a foreign power or an agent of a foreign power reasonably believed to be outside of the United States for national security purposes.[63] The plaintiffs communicated regularly with people likely to be targeted under § 1881a,

57 *Krottner*, 628 F.3d at 1142.

58 *Id.* at 1140.

59 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

60 Clapper *and* Remijas*: A Footnote in the Door for Data Breach Plaintiffs*, 14 MASS TORTS LITIG. 5, 8 (2015).

61 *Clapper*, 133 S. Ct. at 1142.

62 *Id.* at 1157.

63 *Id.* at 1156.

specifically with "people the Government 'believes or believed to be associated with terrorist organizations,' 'people located in geographic areas that are a special focus' of the Government's counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government."[64] Due to these concerns about § 1881a, the plaintiffs stopped engaging in certain telephone and e-mail conversations and used alternative methods of communication, such as traveling abroad to have in-person conversations.[65]

The plaintiffs asserted two separate theories of Article III standing: (1) they would suffer injury because there was "an objectively reasonable likelihood that their communications [would] be acquired under § 1881a at some point in the future," and (2) they had already suffered injury because "the risk of surveillance under § 1881a [was] so substantial that they ha[d] been forced to take costly and burdensome measures to protect the confidentiality of their international communications."[66] Regarding the standing inquiry, this case was significant for two reasons. First, it ruled that the plaintiffs did not sufficiently demonstrate that the potential future injury was imminent.[67] Second, it ruled that any costs incurred by plaintiffs from their efforts to keep their communications confidential did not count towards meeting the standing requirement.[68]

The Court discussed the "highly attenuated chain of possibilities" that would be needed in order for plaintiffs' arguments to prevail:[69]

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the

64 *Id.* at 1145.

65 *Id.* at 1145–46.

66 *Id.* at 1146.

67 *Id.* at 1147.

68 *Id.* at 1155.

69 *Id.* at 1148.

> Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.[70]

Thus, the Court stated the plaintiffs needed to be under surveillance authorized by FISA specifically in order to grant standing. In the Court's opinion, reaching that conclusion required too long of a chain of inferences based on the complaint itself. In addition, the Court stated that even if plaintiffs did suffer the future injury from monitoring, they could not prove that the monitoring was specifically tied to the authorization under FISA.[71] They could have been monitored under the authority of another statute.[72] Thus, with this particular set of facts, the Court seemed to impose a very rigorous standard for standing.

C. The Effect of *Clapper* on Data Breach Cases at the District Court Level

Though *Clapper* did not technically impose more stringent standing requirements or a different doctrine from prior cases, it was widely read as an interpretation of standing doctrine that made it more difficult for plaintiffs to bring suit, especially plaintiffs with claims of future injury.[73] In addition, the subject matter of *Clapper*, data surveillance and future harm, is arguably akin to that of most data breach claims. As such, some courts have used *Clapper* in the context of data breach class actions to dismiss cases upfront. For instance, the United States District Court for

---

70 *Id.*

71 *Id.* at 1149.

72 *Id.*

73 *See* Clapper *and* Remijas*: A Footnote in the Door for Data Breach Plaintiffs*, *supra* note 60, at 8.

the Northern District of Illinois dismissed a data breach class action against Barnes & Noble on standing grounds.[74] *Remijas v. Neiman Marcus Group* was also initially dismissed at the district court level in September 2014.[75] The district court, in making their decision, relied on a reading of *Clapper* as imposing more stringent standing requirements.[76]

Lewert v. P.F. Chang's China Bistro, Inc., the most recent of these three cases, illustrates this interpretation of *Clapper* well. The United States District Court for the Northern District of Illinois ruled that plaintiffs did not meet standing requirements and granted the defendant's motion to dismiss.[77] In a rather curt opinion, the court dismissed all of the plaintiffs' claims, including (1) assertions of overpayment because the services that P.F. Chang's provided were not up to industry standards in terms of data protection; (2) actual losses from unauthorized withdrawals and bank fees; (3) opportunity cost in monitoring credit, obtaining new cards, and losing reward points on cards; and (4) mitigation expenses.[78] The court did not entertain claims about

74 The case involved a data breach in which individuals "potentially stole customer credit and debit information from sixty-three" Barnes & Noble stores, located throughout nine states. *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *1 (N.D. Ill. Sept. 3, 2013). The plaintiffs alleged many injuries, including increased risk of identity theft and time and expense related to monitoring and mitigating this risk. *Id.* at *2. District courts in the Ninth Circuit have adopted a similar approach of distinguishing *Clapper* based on its facts. *See, e.g.*, *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014); *see also* Leon Silver, Andy Castricone & Christina Vander Werf, *Don't Be a Plaintiff's Lawyer's Next Victim: Avoiding the Pitfalls of Data Breach Litigation*, DRI FOR THE DEFENSE, Feb. 2015, at 38.

75 Remijas v. Neiman Marcus Grp., LLC, No. 14-C-1735, 2014 WL 4627893, at *1 (N.D. Ill. Sept. 16, 2014), *rev'd and remanded*, 794 F.3d 688 (7th Cir. 2015).

76 *Id.*

77 In this particular case, plaintiffs alleged injury stemming from a data breach at P.F. Chang's that compromised, by one estimate, seven million cards. Lewert v. P.F. Chang's China Bistro, Inc., No. 14-CV-4787, 2014 WL 7005097, at *1, *4 (N.D. Ill. Dec. 10, 2014).

78 *See generally id.* at *1, *2, *4.

increased risk of identity theft in the future. In quoting *Clapper*, the court said that the harm was not "imminent" because it could take several years to occur, and that "there is no reason to believe that identity theft protection was necessary" after the cancellation of the affected debit card.[79] As such, the court did not believe that the plaintiffs established injury in fact with respect to mitigation damages.[80] In addition, the court made it clear that in some instances the plaintiffs made arguments without sufficiently providing facts or arguments, such as for the opportunity cost of losing a chance to accrue reward points.[81] Perhaps in this case if the plaintiffs' complaint were more detailed, the court would not have dismissed the claims so easily. Nevertheless, this case is an illustration of *Clapper*'s chilling effect on the granting of standing in the Seventh Circuit.[82]

However, there is some variation in interpreting *Clapper* within the Seventh Circuit. For instance, the United States District Court for the Northern District of Illinois found that a plaintiff's allegations of elevated risk of identity theft were sufficient to confer standing in *Moyer v. Michaels Stores, Inc.*[83] It differentiated *Clapper*'s more stringent application of the "certainly impending" standard on the factual context specific to *Clapper*: "(1) national security and constitutional issues and (2) no evidence that the relevant risk of harm had ever materialized in similar circumstances."[84]

Clapper has had virtually no tangible chilling effect on data breach cases in the Ninth Circuit. In the Ninth Circuit, data breach cases are readily analogized to traditional tort claims and standing is generally granted. For instance, in

79 *Id.* at *3.

80 *Id.*

81 *Id.* at *3.

82 Note that the Seventh Circuit reversed and remanded *Lewert v. P.F. Chang's China Bistro, Inc.* recently in April 2016 following the *Remijas* standard. Lewert v. P.F. Chang's China Bistro, Inc., No. 14-3700, 2016 WL 1459226 (7th Cir. Apr. 14, 2016).

83 Moyer v. Michaels Stores, Inc., No. 14-C-561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014).

84 *Id.*

Corona v. Sony Pictures Entertainment, Inc., the District Court for the Central District of California granted standing for a data breach case regarding the exposure of employee information.[85] The district court's reliance on tort law, including product liability class actions, illustrates the fact that these data breach cases can be boiled down to state tort law questions. In this case, for instance, the district court looked to five factors adapted from *Potter v. Firestone Tire & Rubber Co.*, a tort case about exposure to toxic chemicals:

> (1) the significance and extent of the compromise to Plaintiffs' [personally identifiable information]; (2) the sensitivity of the compromised information; (3) the relative increase in the risk of identity theft when compared to (a) Plaintiffs' chances of identity theft had the data breach not occurred, and (b) the chances of the public at large being subject to identity theft; (4) the seriousness of the consequences resulting from identity theft; and (5) the objective value of early detection.[86]

The court found that the plaintiffs' claim of injury due to the necessity of credit monitoring was reasonable considering the fact that the breach caused the public disclosure of Sony employees' sensitive, non-public private personally identifiable information including social security numbers, salary and bank account information, health insurance and other medical information, and visa and passport numbers.[87] Moreover, there was evidence that the hackers shared some of this information online.[88]

---

85 Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600, 2015 WL 3916744, at *3 (C.D. Cal. June 15, 2015). Lead plaintiff Michael Corona sued Sony on behalf of 15,000 current and former Sony employees when the company suffered a data breach. *Id.* at *1; Kurt Orzeck, *Ex-Sony Employees Seek Class Cert. In 'Interview' Row*, LAW360 (July 1, 2015, 4:37 PM), http://www.law360.com/articles/674778/ex-sony-employees-seek-class-cert-in-interview-row [https://perma.cc/TB6V-V5EH].

86 *Corona*, 2015 WL 3916744, at *4 (citing Potter v. Firestone Tire & Rubber Co., 6 Cal. 4th 965, 1008 (Cal. 1993)).

87 *Id.* at *4.

88 *See id.* at *8.

To give an additional example, in *In re Adobe Systems, Inc. Privacy Litigation*, the District Court for the Northern District of California found that the Court's opinion in *Clapper* did not indicate an intention to alter or add to existing standing principles, even though some courts interpreted *Clapper* that way.[89] The district court differentiated the case before it from *Clapper* based on the facts. The Court did not grant standing in *Clapper* because potential future injury was allegedly based on a "highly attenuated" chain of possibilities that did not amount to "certainly impending" injury.[90] In addition, the discussion of standing was in the context of other branches of government potentially violating the Constitution, which made the standing analysis more stringent.[91] In *In re Adobe Systems*, it was clear that the hackers deliberately targeted Adobe's consumer information and seemed to have used Adobe's own software to decrypt the information.[92] The risk of future injury was much more obvious and clearly possible in the imminent future from the facts in *In re Adobe Systems*—the facts indicated a targeted breach and some of the stolen data had already been released online at the time the case was decided.[93]

D. *Remijas*: The Seventh Circuit Case that Granted

89 The Court read *Clapper* in juxtaposition with *Krottner*. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014); *see also* Silver et al., *supra* note 74, at 41. The district court granted standing to the plaintiffs in this case because of the heightened risk of harm due to a 2013 Adobe data breach. *In re Adobe Sys.*, 66 F. Supp. 3d at 1214, 1216; *see also* Silver et al., *supra* note 74, at 41. Defendant Adobe tried to argue that *Clapper* implicitly overruled *Krottner*, but the court disagreed. *In re Adobe Sys.*, 66 F. Supp. 3d at 1212. *Krottner* applied an imminence standard using terms similar to those in *Clapper*. *Id.* at 1214. The court stated that standing was not granted in *Clapper* due to facts that differentiated *Clapper* from *Krottner*, and not due to a difference in law. *See id.*

90 *In re Adobe Sys.*, 66 F. Supp. 3d at 1213.

91 *Id.* at 1214.

92 *Id.* at 1214–15.

93 *Id.* at 1215.

Standing in the Data Breach Context Post-*Clapper*

After *Clapper*, the first court of appeals to consider a data breach case was the Court of Appeals for the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC*.[94] In *Remijas*, the Court of Appeals for the Seventh Circuit granted standing in a data breach class action suit.[95] Several Neiman Marcus customers notified the company of fraudulent charges on their credit cards in December 2013.[96] After an internal inquiry, Neiman Marcus announced that it had been the victim of a cyberattack, with approximately 350,000 cards exposed to malware between July 16, 2013 and October 30, 2013.[97] In response, several consumers brought a class action suit against Neiman Marcus. While the district court ruled that individual plaintiffs and the class lacked standing, on appeal, the Seventh Circuit ruled in their favor with regards to some of their claims.[98]

The plaintiffs asserted two imminent injuries: "an increased risk of future fraudulent charges and greater susceptibility to identity theft."[99] The plaintiffs alleged four injuries already suffered:

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.[100]

Under *Clapper*, claims for future harm can satisfy Article III standing requirements "if the harm is 'certainly impending,' but 'allegations of possible future injury are not

94 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

95 *Remijas*, 794 F.3d at 697.

96 *Id.* at 689–90.

97 *Id.* at 690.

98 *Id.*

99 *Id.* at 692.

100 *Id*.

sufficient.'"[101] Although the district court read *Clapper* as foreclosing use of future injuries to establish Article III standing in data breach situations, the Seventh Circuit read *Clapper* differently.[102] Unlike the facts of *Clapper*, the potential injury—that the plaintiffs' data would be misused—was imminent and real.[103] The court stated that the threat of potential injury was reasonably likely to occur because making fraudulent charges or assuming the plaintiffs' identities was the very reason why hackers stole credit card information from Neiman Marcus in the first place.[104] Thus, at the pleading stage, this court granted standing based on future injury: "an increased risk of future fraudulent charges and greater susceptibility to identity theft."[105]

In terms of harms already suffered, though the court was not convinced by claims (3) and (4), it decided that claims (1) and (2) were sufficient to satisfy the injury-in-fact requirement of Article III standing.[106] The court also held that the other two requirements of Article III standing (causation and redressability) were satisfied.[107] Regarding causation, although one could argue that the hackers obtained the credit card information through other avenues (and potentially not through the malware in Neiman Marcus's system), there was a sufficient enough possibility that Neiman Marcus's malware exposed the information in question for the case to continue.[108] Regarding redressability, although it was true that any fraudulent charges to the plaintiffs' accounts were already reimbursed (via the current credit systems and insurance systems whereby financial institutions and insurers assume liability), redressability

101 *Id*. (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)).

102 *Id*. at 693.

103 *Id*. at 694.

104 *Id*. at 693.

105 *Id*. at 692.

106 *Id*. at 696.

107 *Id*. at 696–97.

108 *Id*. at 696.

was still applicable for "the mitigation expenses or the future injuries."[109] Moreover, there was no guarantee that the injuries plaintiffs suffered or would suffer would be fully reimbursed, due to a variety of restrictions on credit card and debit card liability rules regarding prompt reporting and other variables.[110] Therefore, the court reasoned a favorable court decision would benefit the plaintiffs.[111]

This Seventh Circuit decision echoes some of the existing data breach case law doctrine within the Seventh Circuit and the Ninth Circuit before *Clapper*. It reveals the Seventh Circuit's reasoning and shows that *Clapper*—at least in the Seventh Circuit's view—does not restrict standing in data breach cases. One possible explanation for the Seventh Circuit's reasoning in *Remijas* is the contextual difference between data breaches and foreign intelligence gathering; *Clapper* was a decision based on unique facts. In *Remijas*, the Seventh Circuit took care to distinguish the situation before them from *Clapper* and pointed out the mistake the district court made in its interpretation of *Clapper*.[112] In *Clapper*, the plaintiffs merely suspected that the government intercepted their communications with potential terrorists.[113] The Supreme Court dismissed the case because its claims were too speculative; yet, in so doing, they were still following the "substantial risk" standard.[114] The standard was still in place, though the plaintiffs in *Clapper* were unable to meet it.[115]

In data breach cases generally, the data has already been stolen or compromised because the breach has already occurred. Therefore, the harm is not nearly as speculative as the possibility of surveillance in *Clapper*. The Seventh Circuit argued that the plaintiffs should not have to wait until actual injury or identity theft occurs, since, as the

109 *Id.* at 697.

110 *Id.*

111 *Id.*

112 *Id.* at 693.

113 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1149–50 (2013).

114 *Id.* at 1150, n.5.

115 *Remijas*, 794 F.3d at 693.

Seventh Circuit stated, "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[116] To force plaintiffs to wait until actual identifiable injury occurs would give an undue advantage to potential defendants to argue that the identity theft is not "fairly traceable" to the defendants' data breach.[117]

E. The Third Circuit: A Different Point of View

The Seventh and Ninth Circuit Courts of Appeals have clear positions on plaintiffs' standing in data breach scenarios with respect to increased risk of future harm: increased risk of identity theft is a sufficient injury to meet Article III standing requirements.[118] In contrast, the Court of Appeals for the Third Circuit considers future increased risk of identity theft as insufficient injury to meet the requirements of Article III standing.[119] The Third Circuit fundamentally differs in its approach because of the "speculative nature of any increased risk of future harm" in most data breach cases.[120]

---

116 *Id*.

117 *Id*. (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)).

118 Cave, *supra* note 50, at 774.

119 The Court of Appeals for the First Circuit has also heard a case on data breach. However, the facts of that case differed from the typical data breach suit because the suit was brought preemptively—that is, before any breach occurred. The First Circuit denied standing. *See* Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012). The plaintiff claimed a risk of future harm due to a perceived weakness in data security. *Id.* at 80. Although the First Circuit has not yet decided a case directly analogous to the other cases discussed in this Note, the First Circuit seems more likely to rule in opposition to the Seventh Circuit because the Court held that the lack of a data breach was a fatal omission. *Id.*; *see also* Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1385 (2013).

120 Cave, *supra* note 50, at 776.

In December 2011, in *Reilly v. Ceridian Corp*., the Third Circuit denied standing in a data breach case because the plaintiffs did not satisfy the injury-in-fact requirement.[121] The court found that "allegations of an increased risk of identity theft as a result of the security breach [were] hypothetical, future injuries, and [were] therefore insufficient to establish standing."[122] In so holding, the court distinguished data breach cases from other factual scenarios that would more readily show the risk of future injury (and as such, be able to proceed on the merits) such as defective medical device, toxic exposure, and environmental claims.[123]

The plaintiffs argued before the court that data breach cases should be treated similarly to traditional torts cases for three reasons: (1) they "expended monies on credit monitoring and insurance to protect their safety, just as plaintiffs in defective-medical-device and toxic-substance-exposure cases expend monies on medical monitoring"; (2) "members of this putative class may very well have suffered emotional distress from the incident, which also represents a bodily injury, just as plaintiffs in the medical-device and toxic-tort cases have suffered physical injuries"; and (3) "injury to one's identity is extraordinarily unique and money may not even compensate one for the injuries sustained, just as environmental injury is unique and monetary compensation may not adequately return plaintiffs to their original position."[124] However, the court was not convinced by these arguments because traditional tort cases have two important elements that were missing in this data breach case: an injury that has undoubtedly occurred and the fact that the cases hinge on human health concerns.[125]

Though the weight the court attached to human health concerns is difficult to criticize, there are several weak points in the court's opinion that should have been addressed. First, the idea that an injury has not yet occurred in a data breach

121 Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011).

122 *Id.*

123 *Id.* at 44–46.

124 *Id.* at 44.

125 *Id.* at 45.

context is debatable. The court justified its position by comparing the data breach situation to an exposure to a toxic substance.[126] In a toxic exposure case, the "exposure to a toxic substance causes injury; cells are damaged and a disease mechanism has been introduced" and as such, the harm has already been done though the consequences may not yet be apparent.[127] Despite arguably analogous circumstances in data breach cases, the court was not willing to grant standing in the data breach context. The court seemed to think that medical consequences from toxic exposure were more predictable, while the negative consequences from data breach were not nearly as certain.[128]

The court's analysis of toxic exposure cases shows that standing was granted in these cases though the medical consequences of the toxic exposure were not evident at the time the motion was filed. Similar arguments can also be made in the data breach context: the harm of data breach is analogous to toxic exposure, and the consequences of both are somewhat predictable but perhaps not specifically quantifiable. The court seemed to think that predictability of results is quite high in toxic exposure cases, but perhaps the court put too much weight on the reliability of medical predictions. In other words, to the extent there may be unpredictability in the medical field, there is a similar level of unpredictability in data breaches and the potential fraud that follows. If the court allows standing despite not knowing exactly what medical consequences will flow from toxic exposure, the court should allow standing despite not knowing exactly what identity theft or fraud consequences will flow from a data breach.

126 *Id.*

127 *Id.* (stating "we just cannot yet quantify how it [the harm] will manifest itself" in terms of the development of symptoms or disease). Thus, note that the court conceded that the potential consequences of the initial exposure to toxic substances were not quantifiable. Yet, the court seemed to put greater weight on the predictability of health consequences than harmful consequences from data breaches despite the potential uncertainty in both contexts.

128 *See id*.

The court decided not to grant standing in *Reilly* because the court mischaracterized the harm that is done when data is breached. The court failed to recognize that there was a harm in the breach itself analogous to the first exposure to toxic substances. The court reasoned that the status of data is the same, whether or not it has been exposed:

> In data breach cases where no misuse is alleged, however, there has been no injury—indeed, no change in the status quo. Here, Appellants' credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked. Moreover, there is no quantifiable risk of damage in the future.[129]

In doing so, the *Reilly* court articulated an argument based on a possible misunderstanding about the value of private data. Since no bad act was done yet based on the exposed information, the court presumed that the data was no more vulnerable post-data breach than it was pre-data breach. Yet, post-data breach, regardless of any evidence of misuse of the exposed data, the exposed information is arguably in a different position from information only previously accessible by authorized parties. In other words, the act of exposure can be said to fundamentally change the nature of the information, as privacy has been breached. In short, the Third Circuit did not entertain the possibility that information that is exposed is more vulnerable and somehow altered from the same information properly kept confidential.

Second, the court viewed redressability entirely in monetary terms. It believed that any harm to privacy could be resolved monetarily, which distinguished data breach cases from cases involving human health. However, this distinction may not be legitimate, since in cases involving human health, money is given as a form of redress too. As the court stated when distinguishing data breach cases from environmental claims, "[T]he thing feared lost here is simple cash, which is easily and precisely compensable with a

129 *Id.*

monetary award."[130] Thus, the court's unwillingness to recognize privacy rights was evident, which flows from its mischaracterization of data privacy. One can argue that exposed private information is more likely to be misused than protected private information, which alters and affects the privacy of the information. This type of harm was not captured by the court's analysis.

Though the Third Circuit did not grant standing in *Reilly*, separate charges filed later by the FTC demonstrated that the defendant company, Ceridian, really did fail to secure its customers' personal and financial data and had wrought serious harm.[131] This suggests that perhaps the court should have granted standing in the case to address the potential harm and allow the plaintiffs the opportunity to recover damages. Though an investigation by an administrative agency is not equivalent to a judicial proceeding, it is indicative of a problem potentially worth litigating. As such, this gives additional weight to the argument that standing should have been granted in this case.

IV. THE SEVENTH CIRCUIT'S APPROACH SHOULD BE FOLLOWED, DESPITE PRACTICAL COMPLICATIONS

A. The Seventh Circuit's Approach Is a Step in the Right Direction

The standard of the Seventh Circuit, among current circuit decisions, is the best for plaintiffs and the best for society. It gives plaintiffs the opportunity to address the real harm, injuries, and vulnerabilities experienced by individuals in data breach situations. Data breaches happen too frequently, and affect most, if not all, Americans in some way. Though the courts might not be the ultimate solution to the data breach problem, an approach that utilizes a more

130 *Id.* at 45–46.

131 The company faced an investigation and fines from the FTC. *See* Galbraith, *supra* note 119, at 1383–84 & n.135.

relaxed standing requirement in the data breach context is an effective method to address the data breach problem within the current legal context.

The Seventh Circuit's approach bridges the disconnect between the injury-in-fact standing requirement and allegations of potential future injury by plaintiffs. The Seventh Circuit's ruling in *Remijas* now allows plaintiffs to more easily bring data breach claims.[132] The Seventh Circuit's decision may be the beginning of a shift to thinking about data breach cases as certainly having standing, and victims as suffering the injury of increased risk of future harm. The decision is encouraging, and hopefully will stem the tide of district courts using *Clapper* to deny standing in data breach class actions.

Some commentators have argued in favor of the Third Circuit's approach, since it does not foreclose the possibility of bringing a data breach case based on an increased risk in identity theft.[133] That court signaled in dicta that it might be willing to grant standing if it was clear that the party who committed data breach took personal information, intended to commit future criminal action using this information, and was able to use this information by making unauthorized transactions in the names of data breach victims.[134] Though some commentators say this is consistent with existing standing doctrine, others have argued that these so-called *Reilly* requirements impose too high a bar for plaintiffs.[135] The Third Circuit's test is quite stringent in that it does not leave room for the privacy harm from the exposure of data to be recognized in any form. Ultimately, a discussion of what is private and what is not is essential to tackling the data

132 For instance, following *Remijas*, the Seventh Circuit reversed and remanded a district court decision that had previously denied data breach plaintiffs standing. Lewert v. P.F. Chang's China Bistro, Inc., No. 14-3700, 2016 WL 1459226 (7th Cir. Apr. 14, 2016).

133 Elizabeth T. Isaacs, Comment, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 533 (2015).

134 *Reilly*, 664 F.3d at 42; *see also* Isaacs, *supra* note 133, at 533–34.

135 Isaacs, *supra* note 133, at 534 & n.124.

breach problem head on, as questions of privacy and potential privacy harm underlie all data breach situations. Though the Seventh Circuit's approach does not directly address privacy harm either, its broader reading of standing requirements leaves room for that discussion to take place.

As more class actions are granted standing, more of them have a chance at succeeding on their merits, and companies will be exposed to a greater risk of being liable. Currently, stringent interpretation of standing requirements is a major obstacle to getting consumer victims into court across the board, not just in the realm of data breach cases.[136] Nevertheless, class actions remain a potentially powerful tool for consumers to keep big corporations responsible, since, as Judge Posner has said, "only a lunatic or a fanatic sues for $30."[137] Class actions have traditionally allowed individual victims to band together to challenge improper actions by powerful companies.[138] Utilizing class actions is also a potentially useful vehicle for moving towards regulatory reform, which will eventually be better for companies too. There are historical examples of such shifts, where traditional tort suits led to the creation of an

136 *See* Simon Lazarus, *The Stealth Corporate Takeover of the Supreme Court*, NEW REPUBLIC (Nov. 18, 2015). https://newrepublic.com/article/123984/the-stealth-corporate-takeover-of-the-supreme-court [https://perma.cc/5BER-SEHD]. The article discusses a case in which a credit agency misrepresented the victim's credit history but the plaintiff was not granted standing. *Id.* The court stated that Congress could provide redress only if plaintiff could show something tangible such as a rejection for a job or a loan, and show that furthermore the rejection was due to the credit rating agency's mistaken representation of the plaintiff's credit history. *Id.* In addition, the article discusses a case where workers asking for overtime pay were not able to use basic statistical sampling techniques to show that plaintiffs had suffered injury because they were not paid overtime pay for time spent "donning and doffing" required protective clothing and equipment. *Id.* These are examples of class actions that have been stopped at the courthouse door due to increasingly restrictive interpretations of Article III standing requirements.

137 Carnegie v. Household Int'l, Inc., 376 F.3d 656, 661 (7th Cir. 2004).

138 *See* Lazarus, *supra* note 136.

extensive regulatory framework.[139] For instance, in the food industry context, initial tort litigation was barred by the lack of direct contractual liability between the consumer and the companies that produced food.[140] Yet by the mid-1900s, this barrier was taken away so more tort suits were filed.[141] Facing growing numbers of these challenges from consumers, some companies instituted greater safety regulations on their own.[142] In addition, the modern administrative regulatory state was born to set standards for food safety.[143] Though a direct causal link cannot be found, the increase in suits against food and drug companies and the rise of regulatory bodies for this sector could be related to each other in that the increasing number of suits probably alerted the government to the need for regulation. Thus, class actions can lead to the development of a larger regulatory state that develops, promulgates, and enforces regulations and addresses individual subject matter concerns as they arise. Successful data breach class action suits, and subsequent pushback by companies who have to bear that burden without adequate guidelines, will hopefully generate enough momentum for the federal government to move towards a more comprehensive regulatory solution through which consumers and companies will have clear legal standards.

Though resolving the circuit split by adopting the Seventh Circuit's approach makes the most sense in terms of

139 *See generally, e.g.*, Philip Chen, O'Neill Inst. for Glob. & Nat'l Health Law at Georgetown Univ. Law Ctr., *Appendix B: A Review of Tort Liability's Role in Food and Medical Product Regulation*, *in* INST. OF MED. OF THE NAT'L ACADS., ENSURING SAFE FOODS AND MEDICAL PRODUCTS THROUGH STRONGER REGULATORY SYSTEMS ABROAD 253–64, (Jim E. Riviere & Gillian J. Buckley eds., 2012), http://www.ncbi.nlm.nih.gov/books/NBK 201154/ [https://perma.cc/98UL-78GL] (summarizing the development of food regulation and medical product regulation through pressure from tort suits which allowed suits regardless of a direct contractual relationship between a producer and the consumer-victim).

140 *Id.* at 255.

141 *Id.*

142 *Id.*

143 *Id.* at 254.

beginning to remedy the data breach problem, there are significant practical complications with this approach. These issues are discussed in sections B–E of this Part. Nevertheless, the Seventh Circuit's approach is the most appropriate because it recognizes consumer harm and shifts the potential responsibility onto companies by allowing consumer class actions to litigate substantive issues before a court, rather than stopping them at the door. The company is the appropriate bearer of responsibility in any data breach situation since they are in the best position to address breaches that do occur and prevent future ones from occurring. At the end of the day, this is where the responsibility should lie; it should not be up to the individual consumer victim to resolve the issue when a data breach occurs at a company. The complications that result from adopting the Seventh Circuit's line of reasoning is not an indictment of the approach of the court itself. Rather, they reflect the confused and complicated nature of the state of the law in this field and the need for an ultimate regulatory remedy.

B. Finding Companies Negligent Without a Clear Understanding of What Negligence Means in This Context is Problematic

If data breach cases are increasingly litigated in the courtroom, the outcome and analysis will center on the role and liability of the private company that experienced the breach. A finding that a company is negligent without a clear legal or industry standard is problematic for a variety of reasons. First, companies are currently operating without clear guidance from a set of regulations or best practices.[144]

144 Certainly, potential data safety security standards exist, as discussed briefly in Part II of this Note (such as state and federal regulations, suggested guidelines from agencies, and international sources such as the European Union guidelines or ISO/IEC 27001:2013). *See, e.g.*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/EIC 27001:2013 (2013), https://www.iso.org/obp/ui/#iso:std:54534:en [https://perma.cc/48Z8-2JEL]. The problem lies in the fact that a comprehensive set of

At the end of the day, data breach class actions boil down to a torts negligence action and negligence generally implies a certain standard of care. In the data breach context, however, this is problematic because the acceptable standard is not clear. No one knows what the real standards are beyond a certain baseline level of care (i.e., companies doing a bad job are fairly obvious to spot, but what a good job or an adequate job would look like is not apparent). As such, though courts putting the onus of responsibility on companies makes sense in most instances of data breach, doing so without a clear understanding of what the appropriate duty of care is yet another issue that must be resolved. This is an area ripe for the intervention of standardized regulations.

Currently, given the lack of definitive best practices, directors are probably in the best position to gauge what would be appropriate for their company and their situation.[145] As mentioned above, certain baseline data security standards in the industry are currently discernible despite the lack of standardized regulation, and company management should be proactive in maintaining their own data security systems and paying attention to developments in the field to keep apprised of best data security practices. Because of the current lack of standardization, directors have to fashion these practices for themselves. Moreover, directors should be incentivized to do so not only because of potential damages from class consumer data breach cases, but because of the potential for derivative director and officer suits arising out of data breach incidents.[146] Courts are beginning to interpret the duties of directors to include the investment and management of an effective data security

standardized data security guidelines is not currently enforced on a federal level.

145 Davis et al., *supra* note 29, at 621.

146 Kevin M. LaCroix, *When Data Hacks Lead to D&O Lawsuits, Actual and Threatened,* THE D&O DIARY (Aug. 31, 2015) http://www.dandodiary.com/2015/08/articles/cyber-liability/when-data-hacks-lead-to-do-lawsuits-actual-and-threatened/ [https://perma.cc/J5L6-4HK4].

structure.[147] One such case involved a data breach at Wyndham Hotels and it named ten directors and officers.[148] The case was eventually dismissed, but the court's analysis included a finding that the directors were not grossly negligent in conducting the investigation after the data breach. The court found that: Wyndham's board discussed the cyberattacks during fourteen meetings within the relevant time frame, along with a presentation by the general counsel on the subject at each meeting; the board's audit committee discussed data breach and data security during at least sixteen meetings within the relevant time period; and the company had hired third-party firms to investigate the breach and recommend improvements to Wyndham's systems.[149] As such, some courts seem to require evidence of directors noticing, investigating, and appropriately responding to cyberattacks and data risks. This expectation most likely naturally extends into general data security system management *before* any breach occurs as well. Though these types of suits are not yet commonplace, the attempts to bring such suits indicate a need for a gap of enforcement to be filled. Thus, some principles of the duty of care with regards to data security should be built into the existing corporate regulatory framework.

It is important to note that despite this ambiguity, some data security standards are clearly possible. The European Union already has regulations in place,[150] and the American

147 *See* Michelle A. Reed, Natasha G. Kohne & Jenny M. Walters, *Fiduciary Duties of Directors Are Key to Minimizing Cyber Risk*, NACDONLINE.ORG (May/June 2015), at 41, https://www.akingump.com/images/content/3/6/v2/36491/NACD-article.pdf [https://perma.cc/9EDF-MYG6].

148 Palkon v. Holmes, No. 2:14-CV-01234, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014); *see also* Reed et al., *supra* note 147, at 42.

149 *Palkon*, 2014 WL 5341880, at *5; *see also* Reed et al., *supra* note 147, at 42.

150 *See generally* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014), https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf [https://perma.cc/7K3J-FZRT].

federal government should follow suit. As discussed above, some regulatory agencies, such as the FTC, are already taking on some of that regulatory work.[151] Comprehensive regulatory guidelines are necessary to give companies adequate guidance on best practices for data security, and the FTC may be able to play this role.[152] In *Pisciotta* and *Krottner*, for example, the court found that the companies involved may have been negligent in some way, such as by not using a service that was secure enough for banking applications or not encrypting employee data.[153] In *Remijas*, there were alerts to Neiman Marcus's security system that were triggered when it was compromised.[154] The hackers set off alerts about 60,000 times as they made their way through the network, sometimes setting off hundreds of alerts daily since the card-stealing software was deleted automatically each day from the payment registers.[155] Neiman Marcus claimed that the hackers were sophisticated in giving their malware a name nearly identical to the company's payment software, and indicated that the 60,000 entries over the course of several months represented on average around one percent or less of the daily entries in their protection system.[156] Overlooking these warning signs may be understandable in these circumstances, but this shows that potential data breaches can be flagged. Missing alerts because the malware appeared to be named something very similar to the existing system demonstrates the flaws of data security system design, but it also shows the potential for improvement. In addition, the facts indicate that the internal

151 Cave, *supra* note 50, at 790.

152 Isaacs, *supra* note 133, at 557.

153 Pisciotta v. Old Nat'l Bancorp, 299 F.3d 629, 631–32 (7th Cir. 2007); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140–41 (9th Cir. 2010).

154 Ben Elgin, Dune Lawrence & Michael Riley, *Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data*, BLOOMBERG (Feb. 21, 2014), http://www.bloomberg.com/bw/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data [https://perma.cc/3JMS-Z4YL].

155 *Id.*

156 *Id.*

system worked and alerted the right people (though no action was taken), which means that changes could potentially be implemented so that action is taken earlier on next time.[157] Holding companies accountable to some standard of care is possible, and regulators and courts should aspire to create incentives for companies to do that. Following the Seventh Circuit's approach and allowing standing in more class actions which hold companies accountable will encourage more responsible behavior on the part of companies. Courts are capable of evaluating what data security measures are reasonable and requiring minimum standards at the very least until more comprehensive regulatory measures are put in place.

C. Holding Companies Responsible May Be Problematic When, in Some Cases, Hackings Are Serious Criminal Acts That the Company Could Not Have Reasonably Prevented

Even if companies take action and implement more protections in the future, there is no guarantee that they will be able to combat the sophisticated criminal activity of bad actors. The standard of care should be flexible as the technology evolves. Though private companies should be held accountable to a baseline level of care, addressing cyberattacks and hacking is always going to be a challenge, and the government and private companies will have to work together to come up with a solution. The government is not currently capable of prosecuting criminal hackers abroad effectively in some situations.[158] Data breach is clearly a complicated problem that goes beyond just our borders; individual companies should not have to shoulder that burden alone.

In some cases, sophisticated criminal hackers specifically target companies, and this fact must be recognized. It is unclear whether it makes sense to hold companies liable

157 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

158 *See, e.g.*, Press Release, U.S. Dep't of Justice, *supra* note 44.

when they could not have reasonably prevented particularly sophisticated or malicious attacks. For instance, the 2014 JPMorgan breach was originally thought to be a benign, run-of-the-mill data breach hack because it was not particularly sophisticated.[159] However, federal prosecutors recently uncovered "a trail of [seventy-five] shell companies and a hacking scheme in which the three defendants used [thirty] false passports from [seventeen] different countries."[160] The data breach was a critical component of a wide-ranging criminal enterprise that funneled money from Israel to the United States, through Cyprus, Azerbaijan and Switzerland.[161] This data breach, though not particularly sophisticated on its face, was actually part of a concerted, longstanding criminal plan.[162] As this example shows, data breach cases can often involve more actors and be much more serious than they appear at first glance. Putting the responsibility wholly on the victim company in these instances is most likely unjust and will not help fix the problem.

In addition, some companies that have experienced data breaches recognize the serious nature of the hacking and fight back by suing the hackers. On February 27, 2015, Uber announced that it experienced a data breach and sued an unknown person ("John Doe I") alleging violations of the Computer Fraud and Abuse Act and California's

159 Matthew Goldstein, *4 Arrested in Schemes Said to Be Tied to JPMorgan Chase Breach*, N.Y. TIMES: DEALBOOK (July 21, 2015), http://www.nytimes.com/2015/07/22/business/dealbook/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html?_r=0 [https://perma.cc/C9PJ-BJR8].

160 Liz Moyer, *Prosecutors Announce More Charges in Hacking of JPMorgan Chase,* N.Y. TIMES: DEALBOOK (Nov. 10, 2015), http://www.nytimes.com/2015/11/11/business/dealbook/prosecutors-announce-more-charges-in-jpmorgan-cyberattack.html?src=me&_r=1 [https://perma.cc/YH2C-D8WP].

161 Greg Farrell, *JPMorgan's 2014 Hack Tied to Largest Cyber Breach Ever*, BLOOMBERG BUSINESS (Nov. 10, 2015, 9:31 AM), http://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds [https://perma.cc/KMD4-T3G5].

162 *See id.*

Comprehensive Computer Data Access and Fraud Act in the U.S. District Court for the Northern District of California.[163] "John Doe I" is the stand-in name for the unknown individual or individuals who hacked into Uber's database and downloaded files. So far, the court granted Uber's motions for discovery on a third-party website it believed the hacker used and the Internet service provider of the page in order to attempt to identify the hacker.[164] This also opens the door to questions about whose role it is to track down the hacker—the company has an incentive to do so, but if a cybercrime is committed against the company, the government may have an obligation to do so as well. Private parties should not necessarily have to expend resources to help prosecute this type of crime.

As both targets and victims of data breach, companies are at the center of these crimes. As such, companies are in the best possible position to respond to the data breach problem. Sometimes, companies do everything right by having good data security practices in place and following all the necessary remedial steps available after a breach has occurred. Though this is true in some cases, it is not a relevant concern in the context of granting standing to consumer class action cases on data breach. Consumers should be allowed to get in through the door to litigate the merits of their case because of the harm that they suffered. This harm must be recognized, regardless of whether or not the company might be at fault. The standing requirement in a typical class action case should not bar these facts from coming to light. The company will genuinely not be at fault in some situations, but class actions will allow consumers to seek recourse when that is not the case—when companies are too lax with their data security and have weaknesses in their systems that should have been addressed. Increased litigation will only incentivize companies to be more careful in designing effective data security systems, which is an

163 *Magistrate Dismisses Former Uber Driver's Class Action Over Data Breach*, MEALEY'S LITIG. REP.: CLASS ACTIONS, Nov. 3, 2015, at 23.

164 *Id.*

optimal result for consumers entrusting their data to private companies.

D. Holding Companies Liable May Actually Shift the Costs to Other Institutional Players

The Seventh Circuit's approach may result in more verdicts against companies, but the companies themselves may not be paying the actual costs, meaning the proper parties may not be held accountable. Other entities that private companies work with—such as insurance companies, credit card companies, and banks—might incur the most costs from data breach losses. In fact, holding the company liable does not necessarily incentivize companies to better protect data in those cases, since currently credit card companies and financial institutions are often covering the damages associated with compensating data breach consumer victims in the moments immediately after a breach. These companies often monitor accounts, re-issue new cards, and reimburse for fraudulent charges.[165] Nevertheless, this discrepancy in responsibility shows that there are serious costs associated with data breach, which bolsters the argument for granting standing in data breach cases. Data breach involves clear harms and damages that *someone* has to pay. Allowing more data breach litigation will allow for the companies experiencing the breach to be held liable as a legal matter. As more companies are held liable, the fact that banks, insurance companies, and credit-card companies have to pay out and are affected by data breaches generally will come to light. This will hopefully channel pressure towards a change to the status quo so that companies will be properly incentivized to protect their data.

The complexity of modern credit network relationships means that litigation is an incomplete solution for remedying losses from data breach. This also means that when a merchant company experiences a data breach, the merchant company's costs may be lower than the costs that card-issuing institutions (e.g., banks) have to pay to remedy the

165 Patty, *supra* note 11, at 5–6.

breach and the fraud that follows. Moreover, banks need to cover for breaches experienced by merchant companies in addition to the breaches that they themselves are facing, since financial institutions are targets of hackers as well. To give just one example, JPMorgan announced in October 2014 that its system was breached, with more than 76 million household customer records and seven million business records affected.[166] In addition, banks face additional responsibilities from being in a heavily regulated industry. As such, they face burdens that private merchant companies do not have to shoulder. Furthermore, since clear standards for data protection schemes for merchant companies are not enforced, companies with fairly lax policies can slide by without investing in good data protection.

Currently, the only tangible, significant incentives for companies to prevent data breach are relatively "soft" factors, such as consumer trust, consumer loyalty, and public perception concerns. From this point of view, banks might be footing the bill for companies' negligence in most data breaches. As one commentator stated,

> Financial institutions in the payment card process data chain of custody are subject to various state and federal statutes and regulations concerning data privacy and security, while merchants and other private sector participants elsewhere in the data chain of custody are subject, at least for now, to relatively few data security laws or regulations.[167]

This seems particularly unfair considering that the financial institutions that cover these costs might not even have direct contractual relationships with the company that experienced the data breach.[168] In addition, there are few remedies available to these financial institutions via insurance:

> [W]hen the target of the initial data breach is relatively unregulated, and there is a lack of privity

166 *Id.* at 5.

167 *Id.* at 5.

168 *See id.* at 6.

> of contract between that party and the card-issuing financial institution ultimately burdened by remediation costs and fund losses due to fraud, recovery of damages beyond the limits of any applicable insurance coverage for the card issuer can prove to be a challenge.[169]

Furthermore, large banks, such as JPMorgan, are not the only ones harmed in the context of data breach. Smaller institutions are starting to bring claims against merchant companies that have experienced data breaches as a result of the hardship these smaller banking institutions experience in reimbursing fraudulent transactions or having to provide new credit or debit cards to affected customers.[170] The Credit Union National Association has been active in bringing attention to this problem and advocating for changes in the law that would transfer the burden from financial institutions to the merchant companies.[171]

Recognizing these agency problems and imbalances in responsibility, some states have enacted or are considering statutes that prohibit the retention of payment card data for more than forty-eight hours after transaction authorization, and allow financial institutions to apply for and receive reimbursement from merchant companies utilizing credit card networks that are in violation of the state statutory mandates and who then experience a data breach.[172] This accomplishes the twin goals of regulating merchant companies and holding them responsible for trying to prevent data breach and also relieving financial institutions of their duty to provide remedies to data breach victims by reimbursing victims for fraudulent charges and reissuing cards.

The current imbalance of responsibility is an indication of the problems existing in the current state of affairs, but these state laws balance out the burdens and are an example

169 *Id.* at 6.

170 Thomas Richie, *Data Breach Class Actions*, A.B.A. THE BRIEF, Spring 2015, at 12, 17.

171 *Id.*

172 Patty, *supra* note 11, at 4.

of a possible solution. Companies can be properly incentivized to protect consumer data, for if they fail, they will be penalized with reimbursing other institutional actors. These laws at the state level were a response to the card-issuing banks that had pushed back at having to pay the price for what they perceive as the merchant company's negligence for allowing the data breach to occur in the first place. Allowing more data breach class actions using the Seventh Circuit's recognition of increased risk of future harm will name more companies as responsible, which is significant in its own right. In addition, this will bring more attention to the complexity of the data breach problem, recognize the parties that are truly bearing the burden of data breach, and ultimately will push the system towards a streamlined regulatory solution.

E. Holding Companies Liable Through the Court System Does Not Adequately Address Fundamental Considerations About Privacy

Though the Seventh Circuit's approach is a step in the right direction, merely conferring standing for increased risk of future harm does not adequately recognize privacy harms to the individual. Though there is plenty of case law for addressing physical injuries such as assault and economic harms such as breach of contract, there is no traditional basis for the new losses we experience as a society in the digital age.[173] Standing requirements have become a point of concern for such new, evolving legal protections. Individual data breach victims have tried to address these issues through litigation, but they have often been turned away at the courthouse door. Thus far, no case has decided that data breach, in and of itself, constitutes an injury and confers standing. Nevertheless, the Seventh Circuit's approach at least recognizes the harm of increased risk of future injury,

173 *See* Lexi Rubow, Note, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1010–12 (2014).

which is a step in the right direction for litigating all of the issues related to data breach.

Data breach cases are fundamentally linked to ideas of data privacy. Though overlapping, the two concepts are actually quite different. Unauthorized and broad surveillance of our online activities and communications by government entities and private companies should definitely be of concern. Perhaps the possibility of identity theft, however, is a fact of modern life. The reality is that most data breach cases, even the ones that have been granted standing, do not operate under the assumption that the stolen data or the exposed data itself is a harm worth bringing suit over. The potential for misuse is seen as the actionable harm, but not necessarily the breach itself.

On the one hand, the courts' somewhat lax approach to privacy makes sense—how much of a privacy violation can you claim in good faith in today's hyper-connected world? Does it really matter if a hacker somewhere knows a consumer's name and credit card number? A consumer who experiences exposure of information has the power to render some of that information useless, such as by cancelling the breached credit card and opening a new line. In fact, there are some indications that American consumers "have become numb to breaches altogether, accepting them as a practical inevitability of entering the marketplace," experiencing what one commentator calls "data breach fatigue."[174] At the same time, potentially legitimate privacy concerns are not being addressed because companies are not being held accountable for simply the exposure of this information. Courts should address when mere exposure can itself be harmful and a violation of a privacy right.

Courts currently distinguish amongst different categories of personal identifiable information and weigh their

174 Foresman, *supra* note 23, at 349 & n.56 (citing Sarah Halzack, *Home Depot and JPMorgan Are Doing Fine. Is It a Sign We're Numb to Data Breaches?*, WASH. POST (Oct. 6, 2014, 6:31 PM), https://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/ [https://perma.cc/JSL4-69SD].

comparative value: credit card numbers versus social security numbers, for example. Courts recognize that some information is more private than others. A California magistrate judge in a recent data breach case ruled that the plaintiffs failed to plead sufficient injury because the information stolen was not deemed important enough.[175] This holding came from a situation in which Uber's database, which included the names and driver's license information of its drivers, was hacked by an unknown person.[176] The court examined doctrine in *Krottner*, *Clapper*, and *Reimijas*, and ultimately ruled based on the type of information stolen alleged in the complaint: "[w]ithout a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury."[177]

Data, especially information connected to credit cards, should perhaps be reimagined to fit today's reality. Credit card use is the main mode of commerce and how people operate in the marketplace. This point can cut both ways. To facilitate the ease of electronic transactions, everyone participates in the sharing of information—consumers supply it, and companies read and store it as needed. As such, perhaps all have waived a strong privacy right to this information out of necessity in consenting to and participating in this system. On the other hand, perhaps because everyone uses this mode of payment, personal information should be protected even more rigorously. The number of people at risk is significant, since it encompasses just about everyone who participates in the modern economy. The courts have already begun to think about and discuss the potential consequences of exposure of different types of

175 *See Magistrate Dismisses Former Uber Driver's Class Action Over Data Breach*, *supra* note 163.

176 *Id.*

177 Antman v. Uber Tech., Inc., No. 3:15-CV-01175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015). Also note that though Uber's motion to dismiss was granted, the plaintiff was given twenty-eight days to amend his complaint.

data; surely, they could also think about the different types of privacy harms that could result from the exposure of these varying types of data. It would be an interconnected and analogous issue.

V. CONCLUSION

In sum, the Seventh Circuit's decision in *Remijas* is instrumental in paving the way towards a solution to the data breach problem. The Seventh Circuit granted standing based on victims' reasonable allegations of increased risk of future harms due to data breach.[178] In other words, a circuit court held that claims of potential future damage satisfied the "injury in fact" requirement for the first time after *Clapper*. The Seventh Circuit recently followed its ruling in *Remijas* in deciding to reverse and remand the district court's denial of standing in *Lewert v. P.F. Chang's China Bistro, Inc.*[179] This is particularly significant since *Clapper* chilled the willingness of some district courts to grant standing. The Ninth Circuit has historically followed a similar approach to the Seventh Circuit's reasoning in *Remijas*. In contrast, the Third Circuit does not grant standing based on claims of increased risk of future harm in the data breach context. This circuit split indicates a willingness on the part of some courts of appeals to allow plaintiffs to overcome some of the traditional barriers to litigation for data breach victims. The Seventh Circuit is taking the right step in remedying and recognizing a very real harm—the exposure of private information and the potential harm that can flow from the misuse of it. However,

178 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696–97 (7th Cir. 2015).

179 Lewert v. P.F. Chang's China Bistro, Inc., No. 14-3700, 2016 WL 1459226, at *3 (7th Cir. Apr. 14, 2016) ("[The plaintiffs] describe the same kind of future injuries as the *Remijas* plaintiffs did: the increased risk of fraudulent charges and identity theft they face because their data has already been stolen.").

there are practical consequences to this approach that should be addressed.

Ultimately, the Seventh Circuit's decision signals that the onus of responsibility for data protection should be put on the company. The company is implicitly assigned a duty of care to protect consumer information and employees' personal information. Yet, in some ways this seems unfair since there are no clear regulations on the issue. Moreover, there are some cases in which the company did everything right, but still experienced a breach. It seems unfair to put responsibility on companies when the government has not necessarily been able to prosecute criminals who commit data breach crimes. Furthermore, data breach also involves many different parties, including merchant companies, credit card companies, card-issuing financial institutions, and insurers. Holding the company liable does not necessarily incentivize it to better protect data in some cases, since credit card companies and financial institutions are often covering the damages associated with compensating data breach consumer victims. Lastly, the Seventh Circuit's approach does not adequately address the fact that lawmakers need to consider what data privacy means in today's world, where just about every economic transaction involves the exchange of personal information in some way. The courts have not yet addressed the inherent privacy harm in data breach cases.

Thus, the Seventh Circuit's approach is not without its challenges. It is difficult in application because data breach is a complicated problem. Yet, this approach is necessary in order to apply pressure to the players that matter: private companies. The Seventh Circuit's approach pushes away from the current status quo of data breach law, which favors defendant companies.[180] Only when companies, and by extension, credit card and insurance companies, bear the costs for data breach will broad-based legislation in this arena take form. Ultimately, data breach is probably best

180 *See* Richie, *supra* note 170, at 17.

addressed through a regulatory framework.[181] Change can indeed move in this manner; we have seen this before in history in the food and drug arena.[182] In the area of data breach, the most important changes will likely occur through legislation and regulation.[183]

There may be no need for a whole new agency.[184] A solution can be implemented through an existing body, since companies in the United States are already fairly heavily regulated. The FTC has already taken on this role in some cases.[185] The federal government must set standards for companies to follow to make sure companies are being held accountable for protecting consumer data. These baseline standards should be updated as technology changes. In addition, because of the nature of technology and because of the pervasiveness of data breach occurrences, data security needs to be interwoven as part of the fiduciary duty of company boards of directors. Boards can decide how best to provide for the safety of their data within the context of enforced baseline regulations. Lastly, in addition to a streamlined regulatory approach, this issue requires creative prosecutorial work and international cooperation to target hackers harming American companies from abroad. This is especially important in light of new information showing that some hacks are not the work of a lone wolf, but instead might be part of large conspiracies designed to manipulate markets and execute securities fraud.[186]

Though the direction of the Seventh Circuit in granting standing to data breach victims poses practical challenges that the legal system, the legislature, and private companies are not yet ready to face, it is an essential step in the right

181 Cave, *supra* note 50, at 789–90.

182 *See generally* Chen, *supra* note 139.

183 Richie, *supra* note 170, at 17.

184 Cave, *supra* note 50, at 790.

185 *See* Davis et al., *supra* note 30, at 633; *see also* Richie, *supra* note 170, at 17. There are also indications that the FTC looks favorably upon the *Remijas* decision. *See* Clapper *and* Remijas*: A Footnote in the Door for Data Breach Plaintiffs*, *supra* note 60, at 10.

186 Moyer, *supra* note 160.

direction. As mentioned above, a possible solution to the data breach problem will likely come in the form of a broad, overarching federal regulatory framework. This potential solution, however, is unattainable until more courts follow the Seventh Circuit's approach and readily grant standing to data breach class actions.